Reliability Problems in Nuclear Power Plants Control

MikhailYastrebenetsky
Ukrainian State Scientific
Technical Center on
Nuclear and Radiation Safety
Kharkov, Ukraine
yastreb@online.kharkiv.com

Vyacheslav Kharchenko
Ukrainian State Scientific
Technical Center on
Nuclear and Radiation Safety
Kharkov, Ukraine
V.Kharchenko@khai.edu

Abstract

Factors which define following state of nuclear power plants (NPP) control systems reliability are described. Some undecided tasks are numbered. Two models of NPP control systems reliability are described.

Factors which define following state of NPP control systems reliability

Three main factors influence following state of NPP control systems reliability

1. The accidents on Three Miles Island Nuclear Power Plant –USA and Chernobyl NPP- Ukraine led to considerable toughening of requirements to NPP safety. Reliability of different types of structure, systems and components including control systems (CS) define NPP safety in greater extend.. Therefore

increasing of safety requirements leaded to increasing requirements to CS reliability. It expressed in modification of standard base- international and national of many countries. New international standards, rules and guides were published where were described new requirements to NPP CS reliability (e.g. (IAEA 2002) ,(IEC 2001)). International Electrotechnical Commission has special working group "Reliability of electrical equipment of safety systems " in Technical Subcommittee TK 45A "Reactor Instrumentation"

The main positions of international standards, related to NPP CS reliability:

- obligatory specification of reliability requirements for all systems which have safety classification as safety important;
- regulation of technique of reliability assurance (single failure cr iterion, independence criterion, obligatory of reservation, diversity);
- obligatory demonstration of satisfactory of reliability assurance under regulatory organizations .

2. CS were before analog systems (especially for protection functions). Digital sys tems used the main for information functions. The important step in the progression of NPP CS is arising now from using new information technology .. It appears in:

- complication of NPPCI structure (distribution control, net structures, etc),
- necessary to calculate software reliability as directly in NPP CS, as in instrumental tools for NPP CS design,
- wide using diversity principle for hardware, functions, algorithms and , especially, for software (e.g., using diversity of processors- Intel and Motorola connected with diversity of software-Ada and C++ for NPP "Temelin"- Czeck Republic, designer- Westinghouse-USA) .

3. Besides of existing direction- reliability of industrial control systems ((Cluley 1993), (Yastebenetsky 1989)) new direction arise- reliability of safety critical systems, as rule, digital. Critical systems mean safety importance not only in industry, but in aviation, speed railway transport, military applications, etc. Comparison of methods of safety and reliability

assurance of CS in such heterogeneous applications as NPP and rockets with nuclear weapon shown their sufficient community (Aizenberg 2002).

Current state in Ukraine

The fact that report related NPP reliability was prepared by Ukrainian specialists caused by follow reasons:
- one of the lessons after Chernobyl accident was special attention in Ukraine to NPP CS reliability assurance (especially, protection systems);
- two new units WWER-1000 (Rovno-4 and Khmelnitsky-2) with wide using new computers technique will be commissioned in Ukraine till 2004; there isn't commissioning of new units in USA and West Europe now.

During last years in Ukraine were published three regulations devoted NPP CS which contained the set of positions related reliability:
- requirements to the types and the value of reliability measures (Yastrebenetsky 2000)
- obligatory methods of reliability assurance where the most attention was paid to the methods of contradictions of common cause failures,
- methods CS life extension base on analysis of the trend of failure intensity (Yastrebenetsky 1997)

The main undecided tasks

1.Evaluation of reliability NPP CS software reliability measures and demonstration of adequate software assessment to regulatory organization.
2.Evaluation of reliability of NPP CS with using diversity;
3. Analysis of influence of NPP CS failure to safety violations (this task was decide for violations type as 'reactor core destruction.

New models

Two models of NPPCI are described:
1. The model of system reliability which takes in account hardware and different types of software defects, including different situations depended from the results of the restoration.
2. The model of defects of multiversion NPP CS with direct and indirect diversity metrics /3,4/.

Model 1

NPP CS served reserved system. Their failures can be caused by hardware faults and software defects which appeared not revealed after testing and were showed at the certain input data. At restoration after hardware faults systems come back in an initial condition. At software faults depending on results of restoration some situations are possible:
a) software faults are not eliminated, the system is restarted also a level of non-failure operation software (software faults rate) does not change;
в) software faults are eliminated, new defects are not brought;
c) software faults are eliminated, but there is a probability of entering of new defects at correction software. Hence, change of non-failure operation software after elimination of faults depends from this probability.

It is obvious, that in a case a) the model of system anything essentially does not differ from those models where hardware faults are taken into account only. It is necessary to consider only additional transitions and to estimate the losses of readiness (availability) connected to display of software faults. Software faults rate will depend, first of all, on predicted number of defects in software, their distributions under programs and changes of the input data

In a case в) at performance of the certain conditions (Kharchenko 1999/1) system will be described by multi-fragmental model (MFM). Fragments differ from each other by software faults rate. Parameters of hardware reliability and their influence on avaliability do n ot change. In this model the number of fragments depends on value of change of software faults rate after elimination of next defect.
If to assume, that the value of change of software faults rate is constant, the number of fragments will be fixed. In the report results of MFMs development and research for several typical structures (not reserved and reserved, one-version and multi-version) are submitted.
In other situations (not determined number of software defects, casual influence of corrected defects on rate of their subsequent display, etc.) the model of system essentially becomes complicated and, most likely, transition to imitating (simulation) modelling is inevitable.
For a case c) some variants of the task of the assumptions concerning processes of display, elimin ation and entering of defects which directly influence complexity of models are possible.
Research of systems of considered type is of interest, in our opinion, at use of various kinds of software diversity, the account of parameters of various types of d efects (relative, group, absolute, and also various models of growth of reliability software. The choice and verification of such models can be carried out with use AMA (Assumptions Matrix Assessment) - method (Kharchenko 1999/2).

Model 2

The use of diversity is a radical decision of problem of NPP CSs defence against software defects and decrease of risks of CMF occurrences.
In spite of benefits there are some spe cific problems concerned with using of diversity:
- diversity does not guarantee the absence of coincident errors in different versions;
- diversity may increase summary complexity and cost of CS project; therefore some additional complicated decisions such as the allocation of functions between hardware and software or the type of the voting logic;
- any type of diversity implies a degree of independence; if equipment, software or functional diversity is used, then the claimed level of independence should be de monstrated.
Hence all benefits and drawbacks should be taken into account and the decision by the licensee to use diversity, the choice of type of diversity or the decision not to use diversity should be justified.
The use of these principles is regulated by national and international standards of NPP CS.
The approach to solve the problem is following. The decision to use diversity or not to use diversity commonly is adopted by consideration some qualitative characters of projects. But sometimes we need quantitative data for to draw some conclusions or to choose some design decisions.
Our approach to analysis of NPP CS as multiversion systems (MVS) includes qualitative and quantitative analysis of degree of independence (correlation) of the versions – channels of MVS, reliability and safety assessment of MVS and comparison of characteristics of one -version (primary) system and multiversion system (Kharchenko 2002). Such problems of diversity assessment are typical both for development and e xpert review of NPP CS. The examined approach to diversity assessment is based upon joint use of the following se veral methods:
analysis of design documentation (both system design and system development process) and theoretic - set description of relative, group and absolut e (distinguishable and indistinguishable) defects of versions;
statistic or expert assessment of diversity metrics by use of simulation tools;
probabilistic or deterministic (on a basis of enumeration and analysis of events arose from different type defects) assessment of reliability and safety of one -version and multiversion sy stems.
The proposed technique is used during the expert analysis CS related to safety NPP based on COTS - elements, FPGA-technology, etc.
The following problems are solved in paper.
1. Types of diversity used in NPP CS are analyzed (diversity of hardware, diversity of signals, software diversity, design diversity).

2. Analysis of international and national standards requirements to NPP CS diversity is given.
3. An approach of multiversion systems analysis is proposed. This approach bases on theoretic -set model of components and processes defects.
4. Classification of diversity metrics is considered. It is expedient to divide the set of diversity metrics onto direct and indirect metrics a s per types of evaluated parameters. The firsts of them are the coefficients of distinguishability evaluating a real level and degree of distinction of versions defect components. The seconds ones evaluate a diversity degree of processes of versions develo pment at whole, relying on analysis of phases and sub -phases where diversity was introduced, and assessment of their "weight" as well as "weight" of elements which were undergone to diversity during design, testing, etc.
5. Results of reliability and safet y assessment of MVS with using different metrics are given. The peculiarities of using this measures and metrics for NPP CS expert review are described.

References

Aizenberg A., Yastrebenetsky M (2002). *Comparison of safety assurance principles for carrier rockets and nuclear power plans control systems*. Space Science and Technology. Kiev, pp.55-60.

Cluley J.C. (1994). *Reliability in instrumentation and control*. Butterworth, Heinemann, .155p

IAEA NS-G-1.3. (2002) *Instrumentation and control systems important to safety in nuclear power plants*. Safety guide. Vienna.

IEC 61513. (2001) *Nuclear power plants - instrumentation and control for systems important to safety – general requirements for systems*.

Kharchenko V. (1999/1). *Multiversion Systems: Models, Reliability, Design Technologies*. Proceeding of 10th European Conference on Safety and Reliability, Munich, V.1.

Kharchenko V. (1999/2). *Methods of an Estimation of the Multiversion Safety Systems*. Proceeding of 17th International System Safety Conference, Orlando, USA.

Kharchenko V., Sklyar V. (2001). *The technique of multiversion software and computer control systems simulation*. Information and Control systems for railway transport, n 5.– pp. 17-24.

Kharchenko V., Tarasyuk O., Sklyar V., Dubnitsky V. (2002). *The Method of Software Reliability Growth Models Choice Using Assumptions Matrix*. Proceedings of 26th Annual International Computer Software and Applications Conference (COMPSAC), Oxford, England, Aug., pp. 541-546.

Storey N. (1996). *Safety-critical computer systems*. NY, Addisson-Wesley, 456 p.

Yastrebenetsky M.A. (1989). *Reliability of industrial computer control systems*. Moscow, Energoatomizdat, 264 p. (in Russian).

Yastrebenetsky M., Rozen Yu., Vasilchenko V., Vilkomir S. (2000). *Elaboration of common regulatory requirements on modernized NPP instrumentation and control system important to safety*. Foresight and Precaution. A.A.Balkema, Rotterdam, pp.813-817.

Yastrebenetsky M.,Garagulia L., Gidok G., Goldrin V. (1997). *Life extension of NPP instruments*. The 5th International Conference on Nuclear Engineering (ICONE-5). Book of Abstacts, NY, Nice, France. p.362 .